

10-90, 11-42

FCC Form 481 - Carrier Annual Reporting Data Collection Form

FCC Form 481 OMB Control No. 3060-0966/OMB Control No. 3060-0819 July 2013

<010> Study Area Code 310735
<015> Study Area Name WESTPHALIA TEL CO
<020> Program Year 2015
<030> Contact Name: Person USAC should contact with questions about this data Tina Wieber
<035> Contact Telephone Number: 9895875002 ext.
<039> Contact Email Address: tina.wieber@4wbi.net

Received & Inspected

JUL 02 2014

FCC Mail Room

ANNUAL REPORTING FOR ALL CARRIERS

54.313 Completion Required 54.422 Completion Required

<100> Service Quality Improvement Reporting
<200> Outage Reporting (voice)
<210> Unfulfilled Service Requests (voice)
<310> Detail on Attempts (voice)
<320> Unfulfilled Service Requests (broadband)
<330> Detail on Attempts (broadband)
<400> Number of Complaints per 1,000 customers (voice)
<410> Fixed 0.0
<420> Mobile 0.0
<430> Number of Complaints per 1,000 customers (broadband)
<440> Fixed 0.0
<450> Mobile 0.0
<500> Service Quality Standards & Consumer Protection Rules Compliance
<510> 310735mi510.pdf
<600> Functionality in Emergency Situations
<610> 310735mi610.pdf
<700> Company Price Offerings (voice)
<710> Company Price Offerings (broadband)
<800> Operating Companies and Affiliates
<900> Tribal Land Offerings (Y/N)?
<1000> Voice Services Rate Comparability
<1010> 310735mi1010.pdf
<1100> Terrestrial Backhaul (Y/N)?
<1110>
<1200> Terms and Condition for Lifeline Customers

Price Cap Carriers, Proceed to Price Cap Additional Documentation Worksheet

Including Rate-of-Return Carriers affiliated with Price Cap Local Exchange Carriers

<2000>
<2005>

Rate of Return Carriers, Proceed to ROR Additional Documentation Worksheet

<3000>
<3005>

No. of Copies rec'd 0+3 List ABCDE

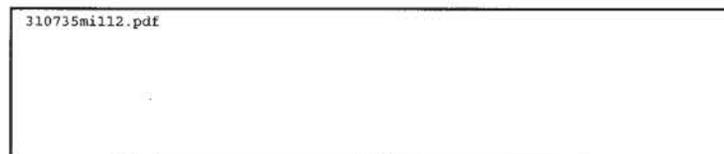
<b>(100) Service Quality Improvement Reporting Data Collection Form</b>	FCC Form 481 OMB Control No. 3060-0986/OMB Control No. 3060-0819 July 2013
---	--

<010> Study Area Code	310735
<015> Study Area Name	WRSTPHALIA TEL CO
<020> Program Year	2015
<030> Contact Name - Person USAC should contact regarding this data	Tina Wieber
<035> Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<039> Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

<110> Has your company received its ETC certification from the FCC?	(yes / no) <input checked="" type="radio"/> <input type="radio"/>
If your answer to Line <110> is yes, do you have an existing §54.202(a) "5 year plan" filed with the FCC?	(yes / no) <input type="radio"/> <input checked="" type="radio"/>

If your answer to Line <111> is yes, then you are required to file a progress report, on line <112> delineating the status of your company's existing § 54.202(a) "5 year plan" on file with the FCC, as it relates to your provision of voice telephony service.

<112> Attach Five-Year Service Quality Improvement Plan or, in subsequent years, your annual progress report filed pursuant to 47 C.F.R. § 54.313(a)(1). If your company is a CETC which only receives frozen support, your progress report is only required to address voice telephony service.



Name of Attached Document

Please check these boxes below to confirm that the attached documents(s), on line 112, contains a progress report on its five-year service quality improvement plan pursuant to § 54.202(a). The information shall be submitted at the wire center level or census block as appropriate.

- <113> Maps detailing progress towards meeting plan targets
- <114> Report how much universal service (USF) support was received
- <115> How (USF) was used to improve service quality
- <116> How (USF) was used to improve service coverage
- <117> How (USF) was used to improve service capacity
- <118> Provide an explanation of network improvement targets not met in the prior calendar year.












(900) Tribal Lands Reporting  
Data Collection Form

FCC Form 481  
OMB Control No. 3060-0986/OMB Control No. 3060-0819  
July 2013

<010> Study Area Code	310735
<015> Study Area Name	WESTPHALIA TEL CO
<020> Program Year	2015
<030> Contact Name - Person USAC should contact regarding this data	Tina Wieber
<035> Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<039> Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

<910> Tribal Land(s) on which ETC Serves

<920> Tribal Government Engagement Obligation

Name of Attached Document

If your company serves Tribal lands, please select (Yes, No, NA) for each these boxes to confirm the status described on the attached document(s), on line 920, demonstrates coordination with the Tribal government pursuant to § 54.313(a)(9) includes:

- <921> Needs assessment and deployment planning with a focus on Tribal community anchor institutions.
- <922> Feasibility and sustainability planning;
- <923> Marketing services in a culturally sensitive manner;
- <924> Compliance with Rights of way processes
- <925> Compliance with Land Use permitting requirements
- <926> Compliance with Facilities Siting rules
- <927> Compliance with Environmental Review processes
- <928> Compliance with Cultural Preservation review processes
- <929> Compliance with Tribal Business and Licensing requirements.

Select (Yes, No, NA)
<input type="checkbox"/>
<input checked="" type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

**(1100) No Terrestrial Backhaul Reporting  
Data Collection Form**

FCC Form 481  
OMB Control No. 3060-0986/OMB Control No. 3060-0819  
July 2013

<010>	Study Area Code	310735
<015>	Study Area Name	WESTPHALIA TEL CO
<020>	Program Year	2015
<030>	Contact Name - Person USAC should contact regarding this data	Tina Wieber
<035>	Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<039>	Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

<1120> Please check this box to confirm no terrestrial backhaul options exist within the supported area pursuant to § 54.313(G)

<1130> Please check this box to confirm the reporting carrier offers broadband service of at least 1 Mbps downstream and 256 kbps upstream within the supported area pursuant to § 54.313(G)

<b>(1200) Terms and Condition for Lifeline Customers</b> Lifeline Data Collection Form	FCC Form 481 OMB Control No. 3060-0986/OMB Control No. 3060-0819 July 2013
--	--

<b>&lt;010&gt;</b> Study Area Code	310735
<b>&lt;015&gt;</b> Study Area Name	WESTPHALIA TEL CO
<b>&lt;020&gt;</b> Program Year	2015
<b>&lt;030&gt;</b> Contact Name - Person USAC should contact regarding this data	Tina Wieber
<b>&lt;035&gt;</b> Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<b>&lt;039&gt;</b> Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

**<1210>** Terms & Conditions of Voice Telephony Lifeline Plans

Name of Attached Document

**<1220>** Link to Public Website

HTTP [http://www.telecommich.org/Documents/WTC-1-complete\\_April\\_2012.pdf](http://www.telecommich.org/Documents/WTC-1-complete_April_2012.pdf)

"Please check these boxes below to confirm that the attached document(s), on line 1210, or the website listed, on line 1220, contains the required information pursuant to § 54.422(a)(2) annual reporting for ETCs receiving low-income support, carriers must annually report:

- <1221>** Information describing the terms and conditions of any voice telephony service plans offered to Lifeline subscribers,
- <1222>** Details on the number of minutes provided as part of the plan,
- <1223>** Additional charges for toll calls, and rates for each such plan.

<b>(2000) Price Cap Carrier Additional Documentation</b> Data Collection Form <i>Including Rate-of-Return Carriers affiliated with Price Cap Local Exchange Carriers.</i>	FCC Form 481 OMB Control No. 3060-0986/OMB Control No. 3060-0819 July 2013
---	--

<b>&lt;010&gt; Study Area Code</b>	310735
<b>&lt;015&gt; Study Area Name</b>	WESTPHALIA TEL CO
<b>&lt;020&gt; Program Year</b>	2015
<b>&lt;030&gt; Contact Name - Person USAC should contact regarding this data</b>	Tina Wieber
<b>&lt;035&gt; Contact Telephone Number - Number of person identified in data line &lt;030&gt;</b>	9895875002 ext.
<b>&lt;039&gt; Contact Email Address - Email Address of person identified in data line &lt;030&gt;</b>	tina.wieber@4wbi.net

**CHECK the boxes below to note compliance as a recipient of Incremental Connect America Phase I support, frozen High Cost support, High Cost support to offset access charge reductions, and Connect America Phase II support as set forth in 47 CFR § 54.313(b),(c),(d),(e) the information reported on this form and in the documents attached below is accurate.**

**Incremental Connect America Phase I reporting**

- <2010> 2nd Year Certification {47 CFR § 54.313(b)(1)}
- <2011> 3rd Year Certification {47 CFR § 54.313(b)(2)}

**Price Cap Carrier Receiving Frozen Support Certification {47 CFR § 54.312(a)}**

- <2012> 2013 Frozen Support Certification
- <2013> 2014 Frozen Support Certification
- <2014> 2015 Frozen Support Certification
- <2015> 2016 and future Frozen Support Certification

**Price Cap Carrier Connect America ICC Support {47 CFR § 54.313(d)}**

- <2016> Certification Support Used to Build Broadband

**Connect America Phase II Reporting {47 CFR § 54.313(e)}**

- <2017> 3rd year Broadband Service Certification
- <2018> 5th year Broadband Service Certification
- <2019> Interim Progress Certification

<2020> Please check the box to confirm that the attached document(s), on line 2021, contains the required information pursuant to § 54.313 (e)(3)(ii), as a recipient of CAF Phase II support shall provide the number, names, and addresses of community anchor institutions to which began providing access to broadband service in the preceding calendar year.

<2021> Interim Progress Community Anchor Institutions

Name of Attached Document Listing Required Information

<010> Study Area Code 310735  
 <015> Study Area Name WESTPHALIA TEL CO  
 <020> Program Year 2015  
 <030> Contact Name - Person USAC should contact regarding this data Tina Wieber  
 <035> Contact Telephone Number - Number of person identified in data line <030> 9895875002 ext.  
 <039> Contact Email Address - Email Address of person identified in data line <030> tina.wieber@4wbi.net

CHECK the boxes below to note compliance on its five year service quality plan (pursuant to 47 CFR § 54.202(a)) and, for privately held carriers, ensuring compliance with the financial reporting requirements set forth in 47 CFR § 54.313(f)(2). I further certify that the information reported on this form and in the documents attached below is accurate.

(3010) Progress Report on 5 Year Plan  
 Milestone Certification (47 CFR § 54.313(f)(1)(i))

Name of Attached Document Listing Required Information

(3011) Please check this box to confirm that the attached document(s), on line 3012 contains the required information pursuant to § 54.313 (f)(1)(ii), the carrier shall provide the number, names, and addresses of community anchor institutions to which began providing access to broadband service in the preceding calendar year.

(3012) Community Anchor Institutions (47 CFR § 54.313(f)(1)(ii))

Name of Attached Document Listing Required Information

(3013) Is your company a Privately Held ROR Carrier (47 CFR § 54.313(f)(2)) (Yes/No)  Yes  No  
 (3014) If yes, does your company file the RUS annual report (Yes/No)  Yes  No

Please check these boxes to confirm that the attached document(s), on line 3017, contains the required information pursuant to § 54.313(f)(2) compliance requires:

(3015) Electronic copy of their annual RUS reports (Operating Report for Telecommunications Borrowers)

(3016) Document(s) for Balance Sheet, Income Statement and Statement of Cash Flows

(3017) If the response is yes on line 3014, attach your company's RUS annual report and all required documentation

Name of Attached Document Listing Required Information

(3018) If the response is no on line 3014, is your company audited? (Yes/No)  Yes  No

If the response is yes on line 3018, please check the boxes below to confirm your submission, on line 3026 pursuant to § 54.313(f)(2), contains

(3019) Either a copy of their audited financial statement; or (2) a financial report in a format comparable to RUS Operating Report for Telecommunications

(3020) Document(s) for Balance Sheet, Income Statement and Statement of Cash Flows

(3021) Management letter issued by the independent certified public accountant that performed the company's financial audit.

If the response is no on line 3018, please check the boxes below to confirm your submission, on line 3026 pursuant to § 54.313(f)(2), contains:

(3022) Copy of their financial statement which has been subject to review by an independent certified public accountant; or 2) a financial report in a format comparable to RUS Operating Report for Telecommunications Borrowers,

(3023) Underlying information subjected to a review by an independent certified public accountant

(3024) Underlying information subjected to an officer certification.

(3025) Document(s) for Balance Sheet, Income Statement and Statement of Cash Flows

310735mi3026.docx

(3026) Attach the worksheet listing required information

Name of Attached Document Listing Required Information

Certification - Reporting Carrier Data Collection Form	FCC Form 481 OMB Control No. 3060-0956/OMB Control No. 3060-0815 July 2015
---	--

<010> Study Area Code	310735
<015> Study Area Name	WESTPHALIA TEL CO
<020> Program Year	2015
<030> Contact Name - Person USAC should contact regarding this data	Tina Wieber
<035> Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<039> Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

**TO BE COMPLETED BY THE REPORTING CARRIER, IF THE REPORTING CARRIER IS FILING ANNUAL REPORTING ON ITS OWN BEHALF:**

<b>Certification of Officer as to the Accuracy of the Data Reported for the Annual Reporting for CAF or LI Recipients</b>	
I certify that I am an officer of the reporting carrier; my responsibilities include ensuring the accuracy of the annual reporting requirements for universal service support recipients; and, to the best of my knowledge, the information reported on this form and in any attachments is accurate.	
Name of Reporting Carrier:	WESTPHALIA TEL CO
Signature of Authorized Officer:	CERTIFIED ONLINE Date 06/30/2014
Printed name of Authorized Officer:	David Fox
Title or position of Authorized Officer:	President
Telephone number of Authorized Officer:	9895875002 ext.
Study Area Code of Reporting Carrier:	310735 Filing Due Date for this form: 07/01/2014
Persons willfully making false statements on this form can be punished by fine or forfeiture under the Communications Act of 1934, 47 U.S.C. §§ 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. § 1001.	

Certification of Agent / Carrier Data Collection Form	FCC Form 481 OMB Control No. 3060-0486/CMB Control No. 3060-0819 July 2013
--	--

<010> Study Area Code	310735
<015> Study Area Name	WESTPHALIA TEL CO
<020> Program Year	2015
<030> Contact Name - Person USAC should contact regarding this data	Tina Wieber
<035> Contact Telephone Number - Number of person identified in data line <030>	9895875002 ext.
<039> Contact Email Address - Email Address of person identified in data line <030>	tina.wieber@4wbi.net

**TO BE COMPLETED BY THE REPORTING CARRIER, IF AN AGENT IS FILING ANNUAL REPORTS ON THE CARRIER'S BEHALF:**

Certification of Officer to Authorize an Agent to File Annual Reports for CAF or LI Recipients on Behalf of Reporting Carrier	
I certify that (Name of Agent) _____ is authorized to submit the information reported on behalf of the reporting carrier. I also certify that I am an officer of the reporting carrier; my responsibilities include ensuring the accuracy of the annual data reporting requirements provided to the authorized agent; and, to the best of my knowledge, the reports and data provided to the authorized agent is accurate.	
Name of Authorized Agent: _____	
Name of Reporting Carrier: _____	
Signature of Authorized Officer: _____	Date: _____
Printed name of Authorized Officer: _____	
Title or position of Authorized Officer: _____	
Telephone number of Authorized Officer: _____	
Study Area Code of Reporting Carrier: _____	Filing Due Date for this form: _____
Persons willfully making false statements on this form can be punished by fine or forfeiture under the Communications Act of 1934, 47 U.S.C. §§ 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. § 1001.	

**TO BE COMPLETED BY THE AUTHORIZED AGENT:**

Certification of Agent Authorized to File Annual Reports for CAF or LI Recipients on Behalf of Reporting Carrier	
I, as agent for the reporting carrier, certify that I am authorized to submit the annual reports for universal service support recipients on behalf of the reporting carrier; I have provided the data reported herein based on data provided by the reporting carrier; and, to the best of my knowledge, the information reported herein is accurate.	
Name of Reporting Carrier: _____	
Name of Authorized Agent or Employee of Agent: _____	
Signature of Authorized Agent or Employee of Agent: _____	Date: _____
Printed name of Authorized Agent or Employee of Agent: _____	
Title or position of Authorized Agent or Employee of Agent: _____	
Telephone number of Authorized Agent or Employee of Agent: _____	
Study Area Code of Reporting Carrier: _____	Filing Due Date for this form: _____
Persons willfully making false statements on this form can be punished by fine or forfeiture under the Communications Act of 1934, 47 U.S.C. §§ 502, 503(b), or fine or imprisonment under Title 18 of the United States Code, 18 U.S.C. § 1001.	

Attachments







# **Westphalia Telephone Company**

## **Five-Year Plan**

### Overview

This plan has been developed for the July 1, 2014 Form 481 filing with the Universal Service Administrative Company (USAC). This is an initial five-year plan forecast for calendar years 2015 through 2019 based on calendar year 2013 actual data. This plan assumes that universal service support revenues will remain unchanged over the 2013 through 2019 years.

Any reliance on this plan is at the reader's own risk because everything from natural disasters to USF reforms and marketplace changes can fundamentally undercut any reasonable expectations in place at the time the plan is submitted.

### General Broadband Requirements

Westphalia Telephone Company (WTC) currently offers broadband service available at rates "reasonably comparable" to offerings of comparable broadband service in urban areas (Par. 91). For example, WTC currently offers 5 mbps downstream with a 1 mbps upstream for \$34.95 per month. In the nearest urban area, Lansing Michigan, AT&T offers 6 mbps downstream with no advertised mbps upstream service for \$34.95 per month.

### Broadband Technical Requirements

WTC has tested their broadband service and determined that the following technical performance characteristics have been measured:

- Minimum actual speeds of 4 mbps downstream and 1 mbps upstream have been achieved at all reasonable feasible customer locations. Actual speed was measured from the end-user interface to the nearest internet access point
- The time it takes for a packet of data to travel from one point in network to another has been tested to be less than 100 milliseconds. Actual latency was measured from the end-user interface to the nearest internet access point.
- WTC currently has a data usage limit of 250 gigabytes per broadband customer per month; however, this usage limit has never been enforced. WTC does not have the equipment to monitor and impose data usage limits and it does not have any plans to buy any such equipment in the foreseeable future.

### Broadband Build-Out Obligations

Upon receipt of a "reasonable request" for service, WTC will deploy services to the requesting customer within a "reasonable time". WTC's goal is to deploy services to a requesting customer in less than a week when it is reasonable. WTC currently deploys "scalable broadband" to their community. Facilities are not always built to meet a single customer request; rather, construction is on a scale which assumes service will be provided ultimately to a broader area surrounding that customer's location.

## Five-Year Build-Out Plan

WTC has one wire center and it is located in Westphalia, MI. For the purposes of this five-year build-out plan, WTC is reporting at the wire center level. The village of Westphalia and the surrounding rural area are included in this wire center. The current population in Westphalia is approximately 925 people and the current population in the surrounding rural area is approximately 1,100. Since WTC meets the minimum broadband standard of 4 mbps downstream and 1 mbps upstream when it is reasonably feasible (this minimum requirement has been met for at least 95% of WTC's customers), there are no plans for major network expansions or upgrades. The two primary components of WTC's plan for the next five years are as follows:

- WTC plans to upgrade peds and cabinets over the next couple years by improving the grounding in them and making them less susceptible to wildlife. The primary reason for the upgrades to peds and cabinets is to increase the reliability of WTC's current broadband service by making it less susceptible to lightning strikes; however, these upgrades may also provide a modest increase to speeds. This could potentially affect all of our customers.
- WTC plans to continue maintenance on the network to ensure that the quality of service remains intact. This could potentially affect all of our customers.

Capital Expenditures	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
2110 Land & General Support					
2210 Central Office Switching					
2230 Central Office Transmission					
2410 Cable & Wire Facilities					

Operating Expenditures	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Plant specific					
Plant nonspecific					
Depreciation and amortization					
Customer Operations					
Corporate Operations					

WTC will continue to assess requests for service for reasonableness and deploy the network in a scalable manner.

**Westphalia Telephone Company is a  
subsidiary of Great Lakes Comnet, Inc. and  
as such is covered by the CPNI Manual and  
the Red Flag Manual of Great Lakes  
Comnet, Inc.**

# CPNI Manual

CPNI Manual

I. DEFINITIONS

II. STATEMENT OF CORPORATE POLICY

III. USE OF CPNI IN GENERAL

IV. GUIDELINES FOR USE OF CPNI

V. OBTAINING CUSTOMER APPROVAL FOR USE OF CPNI

A. Soliciting Customer Approval

B. Use of Opt-Out and Opt-In Approval Processes

VI. NOTICES REQUIRED FOR USE OF CPNI

A. Mandatory Notices Regarding Solicitation

B. Opt-Out Notice Requirements

D. Opt-In Notice Requirements

E. Notice Requirements Specific to One-Time Use of CPNI

VII. COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS

A. Management Safeguards

B. Recordkeeping

C. Authentication and Procedural Safeguards

APPENDIX 1: CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

APPENDIX 2: EMPLOYEE VERIFICATION

APPENDIX 3: SAMPLE OPT-OUT NOTICE

## I. DEFINITIONS

**\*Affiliate\*:** A person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. The term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

**Carrier:** See Telecommunications Carrier.

**CMRS:** Commercial Mobile Radio Service.

**Communications-Related Services:** Telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

**Company:** Great Lakes Comnet, Inc. or Comlink LLC

**Customer:** A person or entity to which a telecommunications carrier is currently providing service.

**Customer Proprietary Network Information (CPNI):** Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. CPNI does not include subscriber list information.

**Customer Premises Equipment:** Equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.

**FCC:** Federal Communications Commission.

**Information Service:** The offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

**Information Services Typically Provided by Telecommunications Carriers:** Information services that telecommunications carriers typically provide, such as Internet access or voice mail services. The term does not include retail consumer services provided using Internet websites (such as travel reservation services or mortgage lending services), whether or not such services might otherwise be considered to be information services.

**Local Exchange Carrier:** Any person engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile service (except to the extent that the FCC determines that such service should be included in the definition of the term).

**Opt-In Approval:** A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain the customer's affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request.

**Opt-Out Approval:** A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the prescribed waiting period, after the customer is provided appropriate notification of the carrier's request for consent.

**Subscriber List Information:** Any information (1) identifying the listed names of a carrier's subscribers and the subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (2) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

**Telecommunications Carrier:** Any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in 47 USC 226).

**Telecommunications Service:** The offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

## II. STATEMENT OF CORPORATE POLICY

The policy of Great Lakes Comnet, Inc. and its wholly owned subsidiary company, Comlink LLC, is to comply with the letter and spirit of all laws of the United States, including those pertaining to CPNI contained in § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's regulations, 47 CFR 64.2001-.2009. The Company's policy is to rely on the involvement of high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

The FCC's regulations, 47 CFR 64.2009, require the Company to implement a system to clearly establish the status of a customer's CPNI approval prior to the use of CPNI, and to train its personnel as to when they are, and are not, authorized to use CPNI, and to have an express disciplinary process in place. This Manual constitutes the Company's policies and procedures related to CPNI.

All employees are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to your immediate supervisor.
- Any violation of, or departure from, the policies and procedures in this Manual shall be reported immediately to the CEO, COO, or the CFO.

## III. USE OF CPNI IN GENERAL

Except as otherwise described in this Manual, when the Company receives or obtains CPNI by virtue of its provision of a telecommunications service, it can only use, disclose, or permit access to individually identifiable CPNI in its provision of:

1. The telecommunications service from which the information is derived; or
2. Services necessary to, or used in, the provision of the telecommunications service, including the publishing of directories.

## IV. GUIDELINES FOR USE OF CPNI

A. The Company may not use, disclose, or permit access to CPNI to market service offerings to a customer that are within a category of service to which the customer does not already subscribe from the Company, unless the Company has customer approval to do so (except that no customer approval is necessary in the situations described in IV.D.).

B. The Company cannot use, disclose or permit access to CPNI to identify or track customers that call competing service providers. Thus, the Company may not use local service CPNI to track all customers that call its local service competitors.

C. The Company may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the Company, without customer approval.

*1. If the Company provides different categories of service, and a customer subscribes to more than one category of service offered by the Company, the Company may share CPNI among its affiliated entities that provide a service offering to the customer, without customer approval.*

*2. If the Company provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except with the customer's approval as discussed in V., below.D. The Company may use, disclose, or permit access to CPNI, without customer approval, as described below:*

1. To provide inside wiring installation, maintenance, and repair services.
2. CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.
3. To market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and Centrex features.
4. For the provision of customer premises equipment and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.
5. To protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.
6. Initiate, render, bill and collect for telecommunications services;
7. Provide call location information concerning the user of a commercial mobile service in emergency situations; and

## V. OBTAINING CUSTOMER APPROVAL FOR USE OF CPNI

### A. Soliciting Customer Approval

The Company may obtain approval through written, oral or electronic methods.

1. 1. If the Company relies on oral approval, it bears the burden of demonstrating that such approval has been given in compliance with the FCC's regulations.
2. 2. A customer's approval or disapproval to use, disclose, or permit access to CPNI must remain in effect until the customer revokes or limits such approval or disapproval.
3. 3. The Company must maintain records of approval, whether oral, written or electronic, for at least one year.

### B. Use of Opt-Out and Opt-In Approval Processes

1. The Company may utilize the opt-out or opt-in method to obtain approval to use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer.

2. The Company may also utilize the opt-out or opt-in method to obtain approval to disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents, to its affiliates that provide communications-related services, and to its joint venture partners and independent contractors.

3. If the Company discloses or provides access to CPNI to a joint venture partner or independent contractor, in addition to obtaining customer approval, it must enter into confidentiality agreements with such contractors or partners. The confidentiality agreement must:

- i. Require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which the Company has provided the CPNI;
- ii. Disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and
- iii. Require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI.

## **VI. NOTICES REQUIRED FOR USE OF CPNI**

### **A. Mandatory Notices Regarding Solicitation**

1. Prior to soliciting any customer approval to use, disclose, or permit access to customers' CPNI, the Company must notify the customer of the customer's right to restrict use of, disclosure of, and access to, the customer's CPNI.
2. The Company must maintain records of the notification, whether oral, written or electronic, for at least one year.
3. Content of Notice: Customer notification must provide sufficient information to enable the customer to make an informed decision whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI. The notification must:
  - i. State that the customer has a right, and the Company has a duty, under federal law, to protect the confidentiality of CPNI.
  - ii. Specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of the right to disapprove those uses, and deny or withdraw access to CPNI at any time.
  - iii. Advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the Company may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. iv. Be comprehensible and not misleading
- v. State that any approval or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.
4. If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.
5. If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.
6. The Company may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. The Company also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.
7. A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.
8. The Company's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

### **B. Opt-Out Notice Requirements**

The Company must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except for one-time use of CPNI, as discussed in VI.E., below). The contents of any such notification must comply with the requirements of VI.A.3., above.

1. The Company must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. The Company may, in its discretion, provide for a longer period. The Company must notify customers as to the applicable waiting period for a response before approval is assumed.
  - i. In the case of an electronic form of notification, the waiting period begins to run from the date on which the notification was sent.
  - ii. In the case of notification by mail, the waiting period begins to run on the third day following the date that the notification was mailed.
2. If the Company uses the opt-out mechanism it must provide notices to its customers every two years.
3. Use of E-mail: If the Company uses e-mail to provide opt-out notices, it must comply with the following additional requirements:
  - i. The Company must have express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;
  - ii. Customers must be able to reply directly to e-mails containing CPNI notices in order to opt-out.
  - iii. Opt-out e-mail notices that are returned to the Company as undeliverable must be sent to the customer in another form before the Company may consider the customer to have received notice; and
  - iv. The subject line of the e-mail must clearly and accurately identify the subject matter of the e-mail.
  - v. The Company must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. The Company may satisfy this requirement through a combination of methods, so long as all

customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

#### **D. Opt-In Notice Requirements**

The Company may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements described in § VI.A.3., above.

#### **E. Notice Requirements Specific to One-Time Use of CPNI**

1. The Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.
2. The contents of any such notification must comply with the requirements of VI.A.3., except that the Company may omit any of the following if not relevant to the limited use for which the carrier seeks CPNI:
  - i. The Company need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election.
  - ii. The Company need not advise customers that it may share CPNI with its affiliate(s) or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party.
  - iii. Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use.
  - iv. Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.
- F. Except for use and disclosure of CPNI that is permitted without customer approval as discussed above, and except for the purpose of marketing communications-related services to a customer, the Company may only use, disclose, or permit access to a customer's individually identifiable CPNI subject to opt-in approval.

### **VII. COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS**

#### **A. Management Safeguards**

1. Training of Company personnel will include review of this Manual by all new employees and all existing employees who have not previously done so.
2. The Company will provide additional training on an as-needed basis.
3. Company personnel will make no decisions regarding CPNI without first consulting one of the following individuals:  
The CEO, COO, or CFO  
The Company's personnel must obtain supervisory approval from a person listed above regarding any proposed use of CPNI.
4. In deciding whether the contemplated use of the CPNI is proper, the individual(s) listed in the previous paragraph will consult this manual, applicable FCC regulations or Compliance Guide, and, if necessary, legal counsel.
5. The person(s) listed in VII.A.3. above will personally oversee the use of approval methods and notice requirements for compliance with all legal requirements.
6. The person(s) listed in VII.A.3. above will also ensure that the Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.
7. Any improper use of CPNI will result in disciplinary action in accordance with established Company disciplinary policies. Any improper use shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. Any company personnel making improper use of CPNI will undergo additional training to ensure future compliance.
8. The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.
  - i. The notice will be in the form of a letter, and will include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.
  - ii. The Company must submit the notice even if the Company offers other methods by which consumers may opt-out.
9. On an annual basis, a corporate officer of the Company will sign a compliance certificate (Appendix 1) stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's rules.
10. The Company will review these procedures on a continuing basis to ensure compliance with all FCC regulations, and will revise these procedures as needed to reflect any subsequent revisions to the applicable Rules and Regulations addressing CPNI.

#### **B. Recordkeeping**

1. The Company will maintain records of its own sales and marketing campaigns that use CPNI in files clearly identified as such. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.
2. The Company will maintain records of its affiliates' sales and marketing campaigns that use CPNI in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.
3. The Company will maintain records of all instances where it discloses or provides CPNI to third parties, or where third parties are allowed

access to CPNI, in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

4. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

5. The Company will maintain separate files in which it will retain any court orders respecting CPNI.

### C. Authentication and Procedural Safeguards

1. Online Access to CPNI. The Company must authenticate Customer without the use of Readily Available Biographical Information or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. Once authenticated, the Customer may only obtain online access to CPNI related to a Telecommunications Service account through a password, as described in Section 10.C.3., that is only prompted by the Company asking for Readily Available Biographical Information, or Account Information.

The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

2. In-Office Access to CPNI. The Company may disclose CPNI (including Call Detail Information) to a Customer who, in the Company's office, first presents a Valid Photo ID matching the Customer's Account Information.

## APPENDIX 1: CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

\_\_\_\_\_ signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of \_\_\_\_\_ Telephone Company (Company). This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide both a Certificate of Compliance and a "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR 64.2001-.2009.

On behalf of the Company, I certify as follows:

1. I am the \_\_\_\_\_ of the Company. My business address is \_\_\_\_\_.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to customer proprietary network information (CPNI).

3. The Company has established a system by which the status of a customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

4. The Company trains its personnel regarding when they are authorized to use CPNI, as well as when they are not authorized to use CPNI. However, Company personnel make no decisions regarding CPNI without first consulting with management. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

5. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

6. The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. Company personnel, prior to making any use of CPNI, must first consult with management regarding the lawfulness of using the CPNI in the manner contemplated. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, the FCC's Compliance Guide, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

8. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith.

9. The Company enters into confidentiality agreements, as necessary, with any joint venture partners or independent contractors to whom it discloses or provides access to CPNI.

10. The Company's policy is to maintain records of customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

Date: \_\_\_\_\_

## APPENDIX 2: EMPLOYEE VERIFICATION

Employee Name: \_\_\_\_\_

Date: \_\_\_\_\_

I have reviewed the Company's Customer Proprietary Network Information Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

\_\_\_\_\_  
Employee Signature

### APPENDIX 3: SAMPLE OPT-OUT NOTICE

\_\_\_\_\_ Company (Company) utilizes Customer Proprietary Network Information (CPNI) when providing telecommunications products and services to its customers. CPNI is defined as information relating to the quality, technical configuration, destination and amount of use of telecommunications services, including information that may appear on a customer's bill. Information published in the telephone directory is not CPNI.

Under Federal law, telephone companies have a duty to protect this information. As a customer, you have the right at any time to restrict the use of CPNI for marketing purposes. This is considered an "Opt-Out" approach. Your approval to use CPNI may enhance the Company's ability to offer products and services tailored to your needs.

The Company proposes to use your CPNI to [Specify: (1) the information that will be used, (2) the specific entities that will receive the CPNI, (3) the purposes for which CPNI will be used].

If you wish to opt-out, you should take the following steps: [list]

Your decision to opt-out will not affect the provision of any services to which you subscribe. The Company does not and will not sell or offer such information to any third party, except as permitted under Federal Communications Commission regulations. Once you opt-out, you will remain on this list until your request otherwise.

If the Company does not receive an opt-out from you prior to the expiration of the 30-day period following the Company's sending of this notice to you, it will assume that you approve of its proposed use of your CPNI.

# Red Flags Manual

Red Flags Manual

SECTION 1:DEFINITIONS

SECTION 2:STATEMENT OF CORPORATE POLICY

SECTION 3:WHAT IS A RED FLAG?

SECTION 4:IDENTIFICATION OF COVERED ACCOUNTS

SECTION 5:OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

SECTION 6:IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

PROTECTION OF EXISTING ACCOUNTS

SECTION 7:PREVENTING AND MITIGATING IDENTITY THEFT

SECTION 8:UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

SECTION 9:ANNUAL REPORT

SECTION 10:SERVICE PROVIDERS

SECTION 11:USE OF CONSUMER REPORTS

SECTION 12:DISCIPLINARY ACTION

APPENDIX 1:ANNUAL REPORT FORM

APPENDIX 2:EMPLOYEE VERIFICATION OF RED FLAG COMPLIANCE MANUAL REVIEW

APPENDIX 3:SAMPLE FORM FOR CREDIT REPORT AUTHORIZATION

## SECTION 1:DEFINITIONS ¶

**Account:** A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

**Annual Report:** See Section 9.

**Board of Directors:** The Company's board of directors, or if the Company does not have a board of directors, a designated employee at the level of senior management.

**Covered Account:** An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

**Consumer Report:** A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 et seq.

**Credit:** The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

**Creditor:** A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit.

**Customer:** A person that has a Covered Account with a Creditor or a financial institution.

**Identity Theft:** A fraud committed or attempted using the Identifying Information of another person without authority.

**Identifying Information:** A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

**Notice of Address Discrepancy:** A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

**Red Flag:** See Section 3.

**Readily Available Biographical Information:** Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

**Service Provider:** A provider of a service directly to a financial institution or Creditor.

## SECTION 2:STATEMENT OF CORPORATE POLICY

The policy of Great Lakes Comnet, Inc. and its subsidiary company Comlink, LLC is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 et seq., and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to Richard Schmoyer, 517-664-1600.
- The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:  
Paul Bowman, CEO  
Richard Schmoyer, CFO  
John Summersett, COO
- The Company's Board of Directors Approved this first revised Manual on October 15, 2009 and replaces the original manual issued in October 2008.

## SECTION 3:WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents.
- Unusual use or suspicious activity related to a Covered Account.
- Presentation of suspicious personal identification information.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

## SECTION 4:IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts, taking into consideration:

- The methods of opening Accounts;
- The methods of access to Accounts; and
- Previous experiences with Identity Theft.

## SECTION 5:OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);
2. Detect Red Flags (see Section 6);
3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and
4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

## SECTION 6:IDENTIFYING RED FLAGS

### OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not open a Covered Account or provide any service until it is able to satisfactorily identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the opening of the Covered Account on hold until it can satisfactorily resolve the Red Flag.

#### A. Opening of Covered Accounts for Personal, Family or Household Purposes.

1. Required Information: When a prospective Customer seeks to open a Covered Account for residential service (i.e., for personal, family or household purposes), the Company will ask for the following from the prospective Customer:

- name;
- address;

- *birth date;*
- *an unexpired government-issued identification bearing a photograph, such as a driver's license or passport. The Company will also encourage (but not require) Customers to establish passwords as a means of protecting against potential future Identity Theft.*

The Company will encourage Customers who establish passwords not to use Readily Identifiable Biographical Information.

## 2. Identification Confirmation.

a. *The Company will make a photocopy of the prospective Customer's identification, and will inspect the identification for any signs of falsification, such as:*

- *misspellings;*
- *a photo that does not resemble the prospective Customer;*
- *inconsistencies in color, texture or images (such as erasures or smudges);*
- *raised edges around a photograph indicating the placement of a second photograph over an original photograph;*
- *card wear inconsistent with date of issuance (such as an identification that appears new but bears an issuance date of many years)*

b. *Address Discrepancies.*

*If a prospective Customer provides an address to the Company that does not match the prospective Customer's identification, the Company will verify the validity of the prospective Customer's address. The following are examples of methods that the Company may utilize:*

- *If the prospective Customer recently moved to the area, the Company will request proof of the recent move.*
- *The Company may choose to order a Consumer Report with respect to the prospective Customer as a tool to confirm identity. Before ordering a Consumer Report, the Company will obtain the prospective Customer's written approval (see Appendix 3). The Company may quiz the prospective Customer regarding non-public information contained therein. The Company may also choose to employ the services of a third-party Identity Theft detection agent.*

c. *The Company will create a record of the means used to verify a Customer's identity. The Company will retain such record until 5 years after the Account is closed. Upon disposal, the Company will completely destroy the record.*

## B. Opening of Business Accounts.

For a prospective business Customer, the Company will require documents to verify the existence of the business. Such documents may include:

- *Articles of Incorporation or Articles of Limited Liability Company and evidence of filing of same with the Michigan Department of Labor and Economic Growth.*
- *Partnership agreement.*
- *Trust instrument. A sole proprietorship may use an "assumed name" document filed with the Department of Labor and Economic Growth, or the personal information of the sole proprietor.*

## C. Examples of Red Flags in the Opening of New Accounts.

### 1. Suspicious Documents and Personal Identifying Information.

- Information on the identification is inconsistent with information provided by the person opening a new Covered Account.*
- Information on the identification is inconsistent with readily accessible information, such as a signature on a check.*
- Documentation that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.*
- An address not matching any address in a Consumer Report;*
- Documents provided for identification appear to have been altered or forged (discussed above).*

### 2. Unusual Use of, or Suspicious Activity Related to, the Covered Account.

- A Covered Account is used in a manner inconsistent with established patterns of activity.*
- Usage of a Covered Account that has been inactive for a reasonably lengthy period of time.*
- A Customer advises that the Customer is not receiving monthly bills from the Company.*
- A Customer advises of unauthorized charges or transactions in connection with a Covered Account.*

3. *The Company receives notice from a Customer, a victim of Identity Theft, law enforcement, or any other person that it may have opened an Account for a person engaged in Identity Theft.*

### 4. If the Company uses a Consumer Report—

- The report contains a fraud or active duty alert.*
- A consumer reporting agency provides a notice of credit freeze in response to a request for a Consumer Report.*
- A consumer reporting agency provides a Notice of Address Discrepancy.*
- A Consumer Report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a prospective*

*Customer.*

*e. A recent and significant increase in the volume of inquiries.*

*f. An unusual number of recently established Credit relationships.*

*g. A material change in the use of Credit, especially with respect to recently established Credit relationships.*

*h. The social security number is associated with a deceased person.*

If a Consumer Report specifies a telephone number to be used for identity verification purposes, the Company will contact the consumer using the specified telephone number.

## **PROTECTION OF EXISTING ACCOUNTS**

The Company has policies and procedures in place to safeguard customer proprietary network information (CPNI). The Company will continue to utilize its CPNI policies and procedures as a safeguard against unauthorized access to Customer CPNI, including pre-texting. Pre-texting is the practice of obtaining call record detail and other CPNI under false pretenses. The Company also monitors suspicious transactions, and verifies change of address requests in accordance with its CPNI Compliance Manual.

The Company updates its Manual to account for changes in law, and it contains all essential information and forms to ensure the Company's compliance with CPNI regulations.

The Company will continue to follow its CPNI Compliance Manual as a means of preventing Identity Theft. The Company will also continue to improve its Identity Theft Prevention Program based on its experience with past incidents of Identity Theft, and new methods of committing Identity Theft of which it becomes aware.

The Company treats the following as Red Flags—

- *Alerts, notifications, or other warnings from consumer reporting agencies or Service Providers;*
- *Suspicious address changes;*
- *The unusual use of, or other suspicious activity related to, a covered Account; and*
- *Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with a Covered Account.*

## **SECTION 7: PREVENTING AND MITIGATING IDENTITY THEFT**

The Company will respond appropriately when it detects a Red Flag. In determining how to respond, the Company will consider aggravating factors that may heighten the risk of Identity Theft.

Appropriate responses include one or more of the following depending on the circumstances:

- *Monitoring a Covered Account;*
- *Contacting the Customer;*
- *Changing passwords or security codes that permit access to a Covered Account;*
- *Reopening a Covered Account with a new account number;*
- *Declining to open a Covered Account for a prospective Customer;*
- *Closing an existing Covered Account*
- *Not collecting on a Covered Account; or*
- *Notifying law enforcement (see Section 10 of CPNI Compliance Manual).*

## **SECTION 8: UPDATING THE IDENTITY THEFT PREVENTION PROGRAM**

The Company will update this Program periodically to reflect changes in risks to Customers or to the safety and soundness of the Company from Identity Theft.

In updating this Program, the Company will consider the following:

- *The Company's experiences with Identity Theft.*
- *Changes in methods with which Identity Theft is committed.*
- *Changes in methods to detect, prevent, and mitigate Identity Theft.*
- *Changes in the types of Accounts that the Company offers or maintains.*
- *Changes in the Company's business arrangements, such as mergers, acquisitions, alliances, joint ventures, and Service Provider arrangements.*

## **SECTION 9: ANNUAL REPORT**

The Company will designate a person to be responsible for preparing an Annual Report to the Board of Directors, appropriate committee of the Board, or a designated senior-level manager.

The Annual Report will address at least the following:

- *The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts.*
- *The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft with respect to existing Covered Accounts.*
- *Arrangements with Service Providers.*
- *Significant incidents involving Identity Theft and management's response.*
- *Recommendations for material changes to the Company's Identity Theft Prevention Program. The Annual Report will be in a format similar to that contained in Appendix 1.*

## SECTION 10:SERVICE PROVIDERS

To the extent that the Company engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the Company will ensure that the Service Provider has its own Identity Theft Prevention Program to detect and address Red Flags.

The Company is ultimately responsible for complying with Red Flag rules even if it outsources Account-related activity to a Service Provider.

## SECTION 11:USE OF CONSUMER REPORTS

To the extent that the Company uses Consumer Reports in the opening of a new Covered Account, it will comply with this Section 11.

If the Company receives a Notice of Address Discrepancy from a consumer reporting agency, the Company must form a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report.

The Company will do one or more of the following to determine whether it has a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report:

- *Compare the information in the Consumer Report with information the Company uses to verify the prospective Customer's identity.*
- *Compare the information in the Consumer Report provided by the consumer reporting agency with information the Company obtains from third-party sources.*
- *Verify with the prospective Customer.*

If the Company has reasonably confirmed that an address relates to the prospective Customer about whom it has requested the report, it must furnish the address for the prospective Customer to the consumer reporting agency from whom it received the Notice of Address Discrepancy.

## SECTION 12:DISCIPLINARY ACTION

Any failure to follow this Manual will result in appropriate disciplinary action in accordance with established Company disciplinary policies. Such failures shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. The Company will also require additional training to ensure future compliance.

## APPENDIX 1:ANNUAL REPORT FORM

To be completed by the Board of Directors, appropriate committee of the Board of Directors, or a designated senior-level manager.

ANNUAL REPORT FOR \_\_\_\_\_

This Annual Report constitutes \_\_\_ Company's (Company) obligation under the Federal Trade Commission's (FTC) regulations and guidelines, 16 CFR Part 681, to produce an Annual Report to address the Company's compliance with the FTC's Red Flag regulations.

### 1. Effectiveness of Policies and Procedures

#### a. Opening of Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts:

#### b. Existing Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with existing Covered Accounts:

### 2. Arrangements with Service Providers

The Company [does/does not] outsource some services to third party Service Providers related to Covered Accounts. [If the Company "does," list them and state:] The Company has taken the following measures to ensure that its Service Provider(s) have Identity Theft Prevention Program(s) to detect and address Red Flags:

### 3. Significant Incidents Involving Identity Theft

The Company reports the following significant incidents involving Identity Theft and management's response:

### 4. Recommendations for Material Changes to the Program

The Company should consider the following changes to its Identity Theft Prevention Program.

[Typed Name]  
[Typed Title]  
Dated: \_\_\_\_\_

## APPENDIX 2:EMPLOYEE VERIFICATION OF RED FLAG COMPLIANCE MANUAL REVIEW

### Employee Verification

Employee Name:

I have reviewed the Company's Red Flag and Address Discrepancies Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

## APPENDIX 3:SAMPLE FORM FOR CREDIT REPORT AUTHORIZATION

### CREDIT REPORT AUTHORIZATION AND RELEASE

Authorization is hereby granted to \_\_\_\_\_ (Company) to obtain a standard factual data credit report through a consumer credit reporting agency chosen by Company.

\_\_\_\_\_  
Social Security Number Date of Birth

\_\_\_\_\_  
Last Name First Name M.I.

\_\_\_\_\_  
Street

\_\_\_\_\_  
City State Zip Code

\_\_\_\_\_  
Phone Number

\_\_\_\_\_  
Signature Date

**(610) Functionality in Emergency Situations**

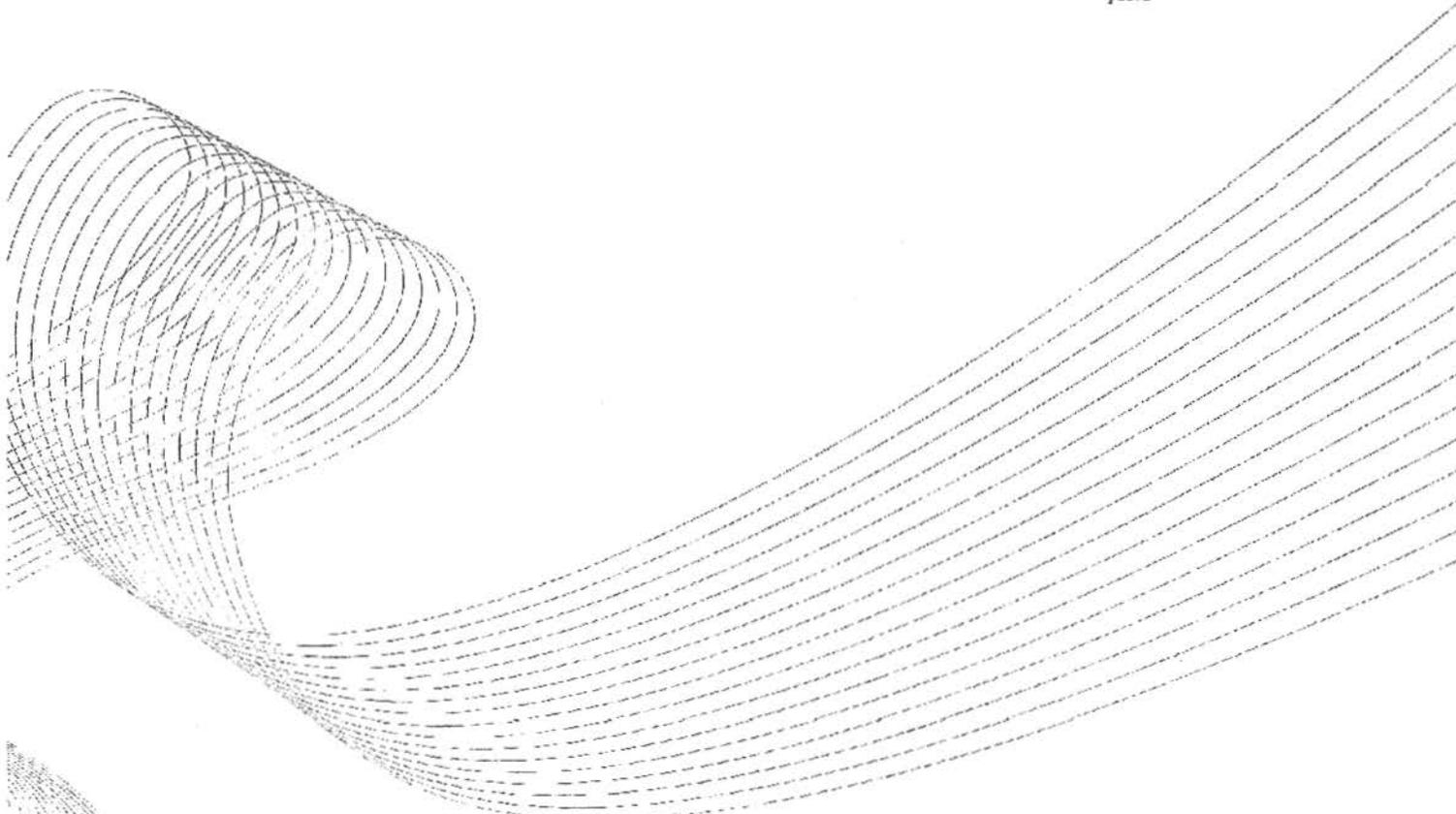
Carrier is able to remain functional in an emergency situation through the use of back-up power to ensure functionality without an external power source. Carrier has backup battery reserve in its central office, which enables it to provide service for a minimum of eight (8) hours. Carrier's service is consistent with the prior obligations to provide service in emergency situations as set forth in §54.202(a)(2) and Rule 46 of the Michigan Public Service Commission's Service Quality Rules (2000 AC, R 484.546), and its network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier has redundancy in its network for use for use in re-routing traffic when facilities are damaged.

**(1010) Descriptive document for Voice Services Rate Comparability**

We certify that Westphalia Telephone's rate of \$22.82 is not greater than two standard deviations above the national average urban rate for voice service (\$46.96).

Westphalia Telephone Company was not provided a management letter for either their 2013 or 2012 audited financial statements. Located on page 26 of this PDF file is the page from the exit memo from our external auditors for the 2013 audited financial statements that is the communication with those charges with governance. Located on page 52 of this PDF file is the page from the exit memo from our external auditors for the 2012 audited financial statements that is the communication with those charges with governance. As you can see, the exit memos are addressed to Great Lakes Comnet. Westphalia Telephone Company is a subsidiary of Clinton County Telephone Company and Clinton County Telephone Company is a subsidiary of Great Lakes Comnet. As such, Westphalia Telephone Company is covered by the Great Lakes Comnet exit memo.

Sincerely,  
David Meyer  
Senior Accountant  
Westphalia Telephone Company  
(517) 664-1900  
dmeyer@comlink.net

A decorative graphic consisting of numerous thin, curved lines that sweep across the page from the left side towards the right. The lines are arranged in a way that creates a sense of motion and depth, starting from a dense, rounded shape on the left and tapering off towards the right.

100 THAT  
years COUNTS

Report of Independent Auditors and  
Consolidated Financial Statements  
With Supplementary Information for

**Clinton County Telephone  
Company and Subsidiaries**

December 31, 2012 and 2011

**MOSS ADAMS** LLP

Certified Public Accountants | Business Consultants

*Acumen. Agility. Answers.*

## CONTENTS

---

	PAGE
REPORT OF INDEPENDENT AUDITORS	1-2
CONSOLIDATED FINANCIAL STATEMENTS	
Consolidated balance sheets	3-4
Consolidated statements of income	5
Consolidated statements of changes in stockholder's equity	6
Consolidated statements of cash flows	7-8
Notes to consolidated financial statements	9-18
SUPPLEMENTARY INFORMATION	
Report of independent auditors on supplementary information	19
Consolidating balance sheet	20-21
Consolidating statement of income	22